On-line Handwritten Signature Verification
A White Paper from Vector Intelligence, Inc.: January, 2002

History

The core of BioSig™, the On-line Handwritten Signature Verification system marketed by Vector Intelligence, Inc. (VII) was developed by Lucent Technologies' Bell Labs. The Bell Labs' project took more than five years of extensive research and development. The size of the research group varied at times from one to four researchers. The effort resulted in several patents, as well as in a highly tested and tuned verification engine code.

VII holds exclusive licenses from Lucent to the signature verification technology, plus a non-exclusive license to technology that provides for secure attachment of handwritten electronic signatures to electronic documents. VII also holds an exclusive license to the signature verification engine's source code developed by Bell Labs.

Patents

The two critical signature verification patents are licensed exclusively to VII.

US 5,828,772: Method and apparatus for parametric signature verification using global features and stroke-direction codes
Signature verification techniques developed by other companies make use of so-called "global" features describing general characteristic of a signature, such as total time to sign. This patent secures the use of a combination of both "global" features of a signature, and "local" signature curve matching, to verify the authenticity of the signer. This technique provides for higher verification accuracy than reliance on global features alone. The local component is described below under "Sophisticated Curve Matching Techniques."

US 5,745,592: Method for detecting forgery in a traced signature by measuring an amount of jitter
This is the second patent controlled exclusively by VII, and focuses on a critical element of forgery detection in handwritten signatures—a forgery created by tracing a signature has much more "jitter" than the original. Jitter is caused by microvibrations of the muscles in the fingers which control the process of handwriting. When a person signs their own signature, these muscles are coordinated and operate fluidly. What Lucent found was that when a forger attempts to copy another's signature, these same finger muscles operate less fluidly and cause the phenomenon of jitter, which can be accurately measured by this patented technology.

US 5,898,156: Validation stamps for electronic signatures
The final patent licensed from Lucent allows VII to engage not only in any signature verification business (as per patent 5,828,772), but also in the business of verifying the authenticity of electronic documents. The combination of these two technologies is critical for any document-oriented applications.

This patent describes a method of verifying that a given handwritten electronic signature was intended for the given electronic document. The technology covered in the patent prevents such forms of deception as the attachment of an authentic signature from one document to a different document.

The patent also thwarts any attempt to fraudulently re-generate a handwritten signature and attach it to another document by re-constructing the timing information in a signature from its geometric shape as sampled by a tablet digitizer. It is oftentimes important to display a signature shape on an unencrypted portion of a document to visually present the signature to a user. However, such an image can present a security threat. The patent covers the entire concept of modifying the geometric characteristics of a signature to hide the signature stroke pattern and speed while preserving the shape of the signature.

Sophisticated Curve Matching Techniques

While the patents cover the key technological bases, a working system requires further perfection of the methodologies described in patents. In particular, very sophisticated curve matching algorithms were developed by Bell Labs to build upon the idea patented in US 5,828,772. As human signatures display a certain amount of variability, it was considered technically challenging to reliably match the proper signature curves. The technical team at Bell Labs experimented with several approaches to curve matching and settled on one which VII believes to be the first curve matching technique reliable enough for commercial deployment.

This new technique, embodied in BioSig™, solves the challenge by generating a "stroke direction code" (or "SDC") from a signature. It does so by subdividing the signature into a sequence of line segments, which Lucent refers to as links, between discrete points along the signature. These links are ordered according to the time-sequence in which the corresponding portions of the signature were made. Each link is assigned a stroke-direction value that depends upon the orientation of that link. The SDC of a signature is the resulting sequence of stroke-direction values.

Sample Signatures Acquisition - Training Process

BioSig™ requires several signature samples from a person to build a signature model for that person. After a sample has been acquired, the system runs several algorithms to extract parameters for the signature model as well as a model of the curve. The process is called training, or enrollment.

Creation of a model is a very fast process and takes well under a second on current generation PCs in single-user mode. Memory requirements are easily within the capabilities of all currently used PC configurations.

On a UNIX platform, "training" speed depends on the hardware configuration of the system as well as on the number of processes competing for system resources. The training process is CPU-intensive. On a UNIX platform the software is implemented as MT-safe library to allow for multiple training requests to be processed simultaneously. VII does not foresee any system degradation in a UNIX environment as the training process happens in realtime, not batch mode, so that computing demands will not typically be concentrated within a specific period of time.

For optimal performance, BioSig™ should be set to generate a model from six signatures. A model may be built from a smaller sample, but verification accuracy may suffer. A sample of more than six signatures usually provides for little improvement over a sample of six.

The software is very robust as to the natural variations in human signatures. However, if a person consistently uses two or more quite different signatures, for example, one with a middle initial and one without, or one with a maiden name and another without one, separate parameter sets (virtual "signature cards") should be created for each one. The training process will reject signatures if they are too dissimilar.

The software is very robust as to the skew of a signing line.

Verification Process

The Verification Process compares a newly submitted signature to the model. A verification score is calculated to determine how closely a newly submitted signature matches the signature description stored in a reference database.*

Depending on the business need or on the amount of money involved in a transaction, the system can be tuned as to false acceptance / false rejection ratio. Although the tradeoff between false acceptance and false rejection is not linear and has a point of overall best performance, certain business conditions may dictate an emphasis on one aspect over the other.

Slightly higher accuracy can be achieved if two signatures are required for verification.

Verification can be accomplished either on the front-end machine or on a central server. Due to security concerns, the front-end verification methodology is better suited to relatively secure environments such as in-store POS terminals.

Like the training process, the verification process is very fast and takes a fraction of a second on current PCs in single-user mode. On a UNIX platform, verification is implemented as MT-safe library.

* Verifying a trial signature involves comparing its feature values to the reference feature values. This comparison is conveniently carried out by computing a total global feature error. This error is obtained by combining (in an appropriate norm) the individual discrepancies between each trial-signature feature value and the corresponding reference value. The total error is compared to a threshold, which is usefully established with reference to deviation measures, such as the standard deviations, of the global features over the group of reference signatures. That is, a larger total error should be tolerated if the global features exhibit a high degree of scatter, than if they show a low degree of scatter.

For verification purposes, an SDC error (which can be combined with the total global feature error) is readily computed by comparing the SDC of a trial signature with an average or representative SDC derived from the reference signatures. We refer to this average or representative SDC as the SDC template.

Verification Accuracy

BioSig™ demonstrates a very high decree of accuracy. It also proves to be very robust in taking into account variance in human handwritten signatures while still distinguishing true signatures from forgeries.

The current version of the software provides for 1% of false rejection rate with 1.3% false acceptance rate with two verification signatures.* For comparison, the best human signature expert has about 33% false acceptance / false rejection rate.

System Requirements - Input Devices

The technology is a software solution, and works with any digitizing tablet that can provide (x,y,t) coordinates where x and y are position coordinates on the digitizer, and t is time. Time does not have to be real time, but should only provide for a consistent presentation of the speed of a pen on the tablet. Substantially all digitizing tablets manufactured today conform to these requirements. These tablets can be either full scale graphics tablets, or other devices such as PDAs (Palm or Pocket PC) or even the small touch pads replicating mouse operations found on most notebook computers.

The technology can also make use of the pressure component of a signature if supported by underlying hardware. However, extensive tests conducted at Bell Labs showed that addition of pressure to the model is more likely to simply increase the noise factor and hence adversely affect the overall false acceptance / false rejection ratio. This is due to the fact that pressure ordinarily varies considerably depending on the posture of the signer, weight of the pen, and other factors unrelated o the identity of the signer.

For a MS Windows-based system front end, VII created a driver that converts input from any Wintab-compatible digitizer into the format required by the system for signature training and verification. Wintab is the current industry standard, and practically all tablets manufactured to work under MS Windows support it.

System Requirements - Storage

The system creates a model of a handwritten signature as a set of parameters extracted from signature shapes and speeds in a training sample. The size of the parameter set can be reduced to 100 bytes.

Models of the signatures can be stored either centrally in any conventional database, or on any other device that has 100 bytes available storage per model, such as a "smart card." A signature model can even fit into the available free storage on a conventional credit card's magnetic strip.

Due to the small size of the parameter set, there should be very little impact on network traffic or on server load in sending a signature over a network for any modern network configurations or server platforms.

* Based on tests run against the Lucent Technologies signature database containing 550 genuine signatures and 325 forgeries from 58 subjects. Tests with similar results were also conducted on NCR databases containing 1772 genuine signatures and 825 forgeries from 145 subjects. However, the NCR database was not available for testing of the latest version of the software.

If graphical representation of a signature is required for some business purposes, that graphical representation usually takes an additional 3K to 5K of storage space. VII also offers "SMP" technology, which stores information about graphical input to a pen or stylus-based computer in a highly-compressed, vector-based format, as a space-saving alternative to bitmapped graphics. Call or write VII for additional information about SMP.

Security

It is not possible to re-create a signature from its model. Thus, storing only models of the signatures is usually advantageous from a security point of view. However, if a graphical representation of a signature is required by business considerations, this representation can be stored together with the model.

Patent US 5,898,156 described above provides a security mechanism to prevent the reconstruction of signature model from a visual representation of a signature.

Standard database security mechanisms provided by every major database vendor, plus properly implemented operations procedures, create additional levels of security for the stored signatures.